AMENDMENT

In the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application. Claims 1-14, 22, 30-31 and 37 were previously canceled. New claims 50-52 have been added. Currently amended claims are shown with additions underlined and deletions in ~~strikethrough text~~. No new matter is added by this amendment.

1.-14. (Cancelled)

15. (Currently Amended) A method, comprising:

receiving at a personal identification device a public key before biometric data associated with enrollment is received;

sending an identifier from the personal identification device to a party based on the public key before biometric data associated with enrollments is received, the identifier being uniquely associated with the personal identification device;

receiving at the personal identification device a digital certificate from the party based on the identifier before biometric data associated with enrollment is received~~, the personal identification device configured to enroll biometric data after the receiving the public key and after the receiving the digital certificate,~~; and

~~disabling functionality within the personal identification device after the receiving the digital certificate until biometric data associated with enrollment is received.~~

disabling functionality within the personal identification device except that the personal identification device is in a wait state associated with future enrollment.

16 (Previously Presented) The method of claim 15, further comprising sending the public key from the personal identification device to the party after the receiving the public key.

17. (Previously Presented) The method of claim 15, wherein the receiving the digital certificate from the party is based on the public key and the identifier.

18. (Previously Presented) The method of claim 15, wherein the identifier is associated with an asymmetric key pair including a personal identification device public key and a personal identification device private key.

19. (Previously Presented) The method of claim 15, further comprising producing the identifier at the personal identification device.

20. (Previously Presented) The method of claim 15, further comprising receiving at the personal identification device the identifier from the party.

21. (Previously Presented) The method of claim 15, wherein the digital certificate includes the public key.

22. (Canceled)

23. (Currently Amended) A method, comprising:

sending a public key to a personal identification device;

receiving an identifier from the personal identification device, the identifier being uniquely associated with the personal identification device;

producing a digital certificate based on the identifier and ~~independent~~before enrollment of biometric data; and

sending the digital certificate to the personal identification device such that functionality of the personal identification device is disabled except that the personal identification device is configured to send the digital certificate to an enrollment party during future enrollment~~configured to enroll initial biometric data after the receiving the digital certificate~~.

24. (Previously Presented) The method of claim 23, wherein the producing of the digital certificate is based, at least in part, on the public key.

25. (Previously Presented) The method of claim 23, wherein the receiving and the producing is performed by a first party, the method further comprising:

receiving at the first party a digital certificate uniquely associated with a second party different from the first party;

adding a public key of the first party to the digital certificate associated with the second party; and

sending the digital certificate associated with the second party from the first party to the second party.

26. (Previously Presented) The method of claim 23, wherein the digital certificate includes the public key.

27. (Previously Presented) The method of claim 23, further comprising producing at the party an asymmetric key pair uniquely associated with the party.

28. (Currently Amended) An apparatus, comprising:

a memory configured to store biometric data of a user;

a processor coupled to the memory and configured to produce a first identifier based on a public key associated with a ~~first~~manufacturer party, the first identifier being uniquely associated with the apparatus, the processor configured to receive a digital certificate from the manufacturer party based on the first identifier, the processor configured to disable functionality of the memory and the processor associated with a party other than an enrollment party~~disable functionality associated with sending biometric data after a digital certificate is received and before biometric data associated with enrollment is received~~;

a biometric sensor coupled to the processor, ~~and~~the biometric sensor configured to read biometric input from the user during enrollment; and

a transceiver coupled to the processor and configured to transmit the first identifier to the ~~first~~manufacturer party and a second identifier to a ~~second~~ party different from the ~~first~~manufacturer party, the second identifier being uniquely associated with the biometric input, the transceiver being configured to receive the digital certificate.

29. (Previously Presented) The apparatus of claim 28, wherein the biometric sensor is a fingerprint sensor configured to read a fingerprint from the user.

30.-31. (Canceled)

32. (Previously Presented) The apparatus of claim 28, wherein the transceiver includes a radio frequency (RF) transmitter.

33. (Previously Presented) The apparatus of claim 28, further comprising a visual display coupled to the processor.

34. (Currently Amended) A method, comprising:

receiving an encryption identifier at a personal identification device from a party during pre-enrollment;

receiving a digital signature at the personal identification device from the party, during pre-enrollment;

the encryption identifier and the digital signature collectively configured to enable verification of the partypersonal identification device by the personal identification deviceparty, the personal identification device configured to enroll biometric data after the receiving the encryption identifier and after the receiving the digital signature; and

disabling functionality within the personal identification device after the receiving the digital signature and before biometric data associated with enrollment is received.

disabling functionality within the personal identification device except for functionality associated with future enrollment.

35. (Previously Presented) The method of claim 34, wherein:

the encryption identifier is a public key; and

the receiving the digital signature including receiving a digital certificate including the digital signature.

36. (Previously Presented) The method of claim 34, wherein:

the encryption identifier is a public key; and

the receiving the digital signature including receiving a digital certificate including the digital signature based on the public key.

37. (Canceled)

38. (Previously Presented) The method of claim 15, wherein the party is a manufacturer of the personal identification device and separate from an enrollment party authorized to enable enrollment of the biometric data at the personal identification device.

39. (Previously Presented) The method of claim 15 wherein the party is a first party, the personal identification device being configured to enroll the biometric data from a second party different from the first party after the receiving at the personal identification device the digital certificate.

40. (Currently Amended) The method of claim 15, wherein the digital certificate includes data associated with the personal identification device ~~and excludes biometric data~~.

41. (Currently Amended) The method of claim 23, wherein the public key is associated with a manufacturer of the personal identification device and separate from ~~an~~the enrollment party authorized to enable enrollment of the biometric data at the personal identification device.

42. (Currently Amended) The method of claim 23, wherein the personal identification device is configured to enroll ~~the initial~~ biometric data from ~~an~~the enrollment ~~authority~~party after the sending the digital certificate.

43. (Currently Amended) The method of claim 23, wherein the producing the digital certificate is based on data associated with the personal identification device ~~and excluding biometric data~~.

44. (Currently Amended) The apparatus of claim 28, wherein the transceiver is configured to receive the digital certificate from the ~~first~~manufacturer party.

45. (Currently Amended) The apparatus of claim 28, wherein ~~the first party is a manufacturer of the apparatus,~~ the ~~second~~ party is an enrollment authority of the biometric data.

46. (Currently Amended) The apparatus of claim 28, wherein the digital certificate includes data associated with the apparatus ~~and excludes biometric data~~.

47. (Previously Presented) The method of claim 34, wherein the party is a manufacturer of the personal identification device.

48. (Previously Presented) The method of claim 34, wherein the party is a first party, the personal identification device being configured to enroll biometric data from a second party different from the first party after the receiving the encryption identifier and after receiving the digital certificate.

49. (Currently Amended) The method of claim 34, wherein the digital signature includes data associated with the personal identification device ~~and excludes biometric data~~.

50. (New) The method of claim 15, wherein the wait state associated with future enrollment is a first wait state associated with future enrollment.

51. (New) The method of claim 23, wherein the future enrollment is a first future enrollment.

52. (New) The method of claim 34, wherein the future enrollment is a first future enrollment.